



**Tempest**

**ACADEMY**  
**CONFERENCE < 2024 >**





## O Tempest Academy Conference é mais um recurso ofertado dentro do Programa ACTION Talents, visando:

- Contribuir com Professores e Estudantes no processo de formação profissional, através da disseminação e compartilhamento de conhecimento técnico em cibersegurança;
- Realizar o mapeamento e atração de Talentos profissionais em cibersegurança;
- Apresentar à comunidade acadêmica: o mindset, a realidade profissional e o ambiente dos eventos da comunidade de cibersegurança.

**PÚBLICO ALVO:** Estudantes e Professores(as) dos cursos de graduação, pós-graduação e ensino técnico de todo o País.

**FORMATO:** O evento será realizado nos dias **8 e 9/Nov/2024**, no formato **HÍBRIDO** - Presencial ou Remoto (Online).

- Presencial: Universidade São Judas – Móoca: Rua Taquari, 546, Móoca, São Paulo/SP. CEP: 03166-000, ou;
- Remoto (Online): via videoconferência do Zoom. Os links de acessos serão disponibilizados no Even3 e também por e-mail.

### ATIVIDADES & PROGRAMAÇÃO:

- Keynote Speakers
- Palestras Técnicas
- Minicursos Técnicos
- Ask the Experts
- CtF - Capture the Flag: Competição com Premiações
- CyberSec Jobs: Feira de Empregabilidade para Talentos
- Reunião de Professores(as) do ACTION Talents
- Coquetel e Atividade Social de Integração

## Dia 1 (8/Nov - Sexta-Feira)

Minicursos		Palestras					Outras Atividades		Competição				
Offensive	IA/DS/ML	Offensive	Defensive	Threat Intel	Infra, Cloud & IoT	Eng.Soft & AI/DS/ML	CyberSec Jobs						
C R E D E N C I A M E N T O													
8:00													
8:30													
ABERTURA DO EVENTO: Gerson Castro (Tempest, Head of Academy, Research & Publishing)													
9:00													
Keynote Speaker: <b>Marcelo José Ruv Lemes (Embraer, Senior Software Specialist, PhD)</b>													
9:30													
O desenvolvimento de software nos produtos Embraer: História e Desafios.													
10:00													
<b>Introdução à Web Application Security para Futuros Pentesters</b> Gabrielle Delgado & Jéssica Giuot (Tempest)	<b>Empowering Intrusion Detection Systems with Machine Learning</b> Paulo Waitana & Julio Luz (Tempest)	<b>CyberSec Jobs: Oportunidades do Programa de Especialização em Software da Embraer - Marcelo Ruv &amp; Convidados/Embraer</b>						<b>Ask the Experts</b>	<b>Capture the Flag (CTF)</b>				
		INTERVALO								Atividades nos Stands			
		Cross-Site Script Inclusion - <b>Henrique Curi</b>	"O Alvo: Identidade Siliada" - <b>Rivaldo Oliveira</b>			Do virtual ao chão de fábrica: desvendando segurança em TI e TO - <b>Prof. Wagner Rodrigues/SENAI SP</b>	O Impacto da Inteligência Artificial Generativa em Resolver Issues de Código em Ambientes DevSecOps - <b>Prof. Cesar Marcondes/ITA</b>			<b>Embraer:</b> Roda de Conversa - <b>Carlos Guerra, Manuela Souza e Iraline Nunes/Embraer</b>			
		12:00											
		12:30											
		13:00											
		13:30											
		14:00											
		14:30											
		15:00											
15:30													
16:00													
16:30													
17:00													
17:30													
18:00													
18:30													
19:00													

Atividade Social de Integração (Happy Hour): DJ e Comes &amp; Bebes

Programação sujeita a alterações sem aviso prévio.



Dia 2 (9/Nov - Sábado)										
Offensive			Palestras					Outras Atividades		Competição
Offensive	Threat Intel	CloudSec	Offensive	Defensive	Threat Intel	Infra, Cloud & IoT	Eng.Soft & AI/DS/ML	CyberSec Jobs		
8:00										
8:30										
9:00	Keynote Speaker: <b>Ineida Moura (Itaú, Gerente de Segurança da Informação)</b>									
9:30	A Segurança da Informação muito além de Ataque e Defesa									
10:00	CyberSec Jobs: Roda de Conversa: Cultura & Carreiras - <b>Ineida Moura &amp; Convidados/Itaú</b>								Atividades nos Stands	
10:30	INTERVALO									
11:00	Como o acaso nos ajuda a encontrar vulnerabilidades: AFL++ e uma introdução a Feedback-Based Fuzzing - <b>André Bermudes</b>	Perspectivas para o cenário de inteligência cibernética - <b>Daniel Nering/Itaú</b>	O que podemos descobrir sobre um binário só olhando pra fuça dele - <b>Fernado Mercês/Mente Binária</b>	Wi-Fi além da conectividade: detecção de intrusos e autenticação biométrica: <b>Prof. Lourenço Pereira/ITA</b>						
11:30										
12:00	<b>A L M O Ç O</b>									
12:30										
13:00										
13:30	Introdução à Engenharia Reversa de Software - <b>Gustavo Carvalho (Tempest)</b>	OpenCTI: Fortalecendo a Segurança com Threat Intel - <b>Prof. J. Aragão (CIMATEC/BA)</b>	Intro a CloudSecurity na plataforma Google Cloud - <b>Prof. João Leite (ABRedes   Matza)</b>	Da segurança ofensiva à defensiva: dissecando um ataque - <b>Vanessa Bandeira</b>	Desvendando a Cadeia de Ataque: Uma Jornada Através do Processo Investigativo de um ataque de Dupla Extorsão - <b>Ricardo Jesus</b>	Desafios na mensuração de riscos cibernéticos - <b>Roberta Costa</b>	Subvertendo Modelos de Machine Learning com Ataques Adversariais - <b>Paulo Matana</b>			
14:00				Hack the Future: Construindo uma Carreira e Mindset em Offensives Security - <b>Prof. Rafael Santos/FIAP</b>	Desmistificando o Trojan Bancário - Conflito Bélico de Tróia - <b>Lucas Souza</b>	Validação eletrônica no Brasil: desafios, perspectivas e resultados da colaboração entre TSE e academia - <b>Prof. Marcos Simplicio/USP</b>	NLP & Assistentes Virtuais: Voz Entendendo na prática o funcionamento por trás da Alexa - <b>Douglas Oliveira</b>	Atividades nos Stands		
14:30										
15:00	INTERVALO									
15:30										
16:00	Kerberos: authentication in corporate environments - <b>José Edgar Baccarat</b>	APT Groups & Threat Actors no setor Aeroespacial Brasileiro - <b>Rodrigo Rios</b>	Engenharia Social: A Arte de Manipular e Como se Proteger - <b>Cleber Castro</b>	O poder da simplicidade na era hiperconvergente - Por que complicar, se o arroz com feijão ainda sustenta? - <b>Prof. Luciano Peraro/CPS ETEC</b>					Tempest: Papo de Carreira <b>Roberto Alexandre &amp; Convidados/Tempest</b>	
16:30										
17:00										
17:30	Matrix da Mentira: Como informações manipuladas distorcem a realidade - <b>Matheus Pessoni</b>								O Vale da Estranheza à Conquista da Cibersegurança: Formação, Talentos e Mindset na Era da Inteligência Artificial. <b>Prof. Olivia Braga/FIAP</b>	Atividades nos Stands
18:00	ENCERRAMENTO DO EVENTO									

Programação sujeita a alterações sem aviso prévio.



Palestras				
Keynotes Speakers				
Data	Hora	Título Palestra	Palestrante	Descrição da Palestra
08/Nov (Sex)	9:00	<b>Abertura do Evento</b>	<b>Gerson Castro</b> Head of Academy, Research & Publishing Tempest	Boas vindas, apresentação do objetivos & orientações gerais sobre a programação do evento, com participações especiais.
	9:30	<b>KEYNOTE:</b> <b>Contexto da CyberSec x Embraer e suas Oportunidades</b>	<b>Marcelo José Ruv Lemes</b> Senior Software Specialist, PhD Embraer	A palestra abordará a evolução do desenvolvimento de software embarcado nas aeronaves produzidas pela Embraer e os principais desafios em cada projeto.
	14:00	<b>KEYNOTE:</b> <b>Cibercrime no Brasil: Audácia e criatividade andando lado a lado</b>	<b>Aldo Albuquerque</b> Executive Vice President Tempest	O intuito dessa palestra será o de apresentar como vem trabalhando os cibercriminosos no Brasil. A partir alguns interessantes casos/exemplos reais de golpes e fraudes, será demonstrado o quão avançadas estão as técnicas utilizadas atualmente pelos criminosos brasileiros, exibindo um cenário diverso e criativo, com uso pesado de técnicas de engenharia social, automação, oportunismo e uma pitada do "jeitinho brasileiro".
09/Nov (Sab)	9:00	<b>KEYNOTE:</b> <b>A Segurança da Informação muito além de Ataque e Defesa</b>	<b>Ineida Moura</b> Gerente de Segurança da Informação Itaú	Imagine um cenário em que a Segurança da Informação não se resume apenas a proteger sistemas contra ataques, mas também a melhorar a experiência do usuário? Nessa palestra vamos explorar como a segurança pode ir além das barreiras técnicas e se transformar em um diferencial competitivo. Você já parou para pensar em como os produtos de segurança impactam a vida do usuário? E como garantir que eles sejam não apenas eficazes, mas também intuitivos e agradáveis de usar? Nessa sessão, vamos discutir como integrar a experiência do cliente ao design de produtos de segurança, desde o início do processo, criando soluções que inspirem confiança e satisfação. Venha discutir como unir segurança e usabilidade, quebrando paradigmas e trazendo um novo contexto para Segurança da Informação
	18:30	<b>Encerramento do Evento</b>	<b>Gerson Castro</b> Head of Academy, Research & Publishing Tempest	Divulgação & Premiação dos Vencedores do Capture the Flag (CTF); Sorteios e Agradecimentos finais.



Tempest

ACADEMY  
CONFERENCE <2024>

## Tempest Academy Conference 2024 | Palestras Técnicas

### Trilha: **Offensive Security**

Data	Hora	Título Palestra	Palestrante	Descrição da Palestra
08/Nov (Sex)	11:30	<b>Cross-Site Script Inclusion:</b> um estudo das estratégias de mitigação e atual prevalência da vulnerabilidade em navegadores	<b>Henrique Curi</b> Tempest	A palestra apresenta um estudo da vulnerabilidade Cross-Site Script Inclusion (XSSI) e os cenários de exploração em navegadores atuais, além de uma estratégia de mitigação baseada em cookies. Fortemente negligenciada, tanto por desenvolvedores quanto pesquisadores de cibersegurança, esta vulnerabilidade ainda representa fonte de ameaça para indivíduos e negócios.
	15:30	<b>Engenharia reversa aplicada para debug</b>	<b>Prof. Carlos Noriega</b> São Judas/SP	Será uma exemplificação sobre o conceito de engenharia reversa e imediatamente depois passaremos a usar uma ferramenta específica para realizar um debug em assembly encontrando uma mensagem secreta e depois, também com assembly, como encontrar uma senha em um executável (.exe). A ideia é apresentar conceitos rápidos sobre debugging com assembly e engenharia reversa.
	17:00	<b>Explorando uma misconfig da Checkpoint</b>	<b>Antonio Junior</b> Tempest	Durante a exploração de uma vulnerabilidade de configuração incorreta implementada no Checkpoint, foi possível burlar uma regra de segurança da VPN utilizando uma falha na validação do lado do cliente (client-side).
	18:00	<b>HTTP Request Smuggling:</b> Explorando Vulnerabilidades entre Servidores Web	<b>Ariel Tarabori</b> Tempest	Nesta apresentação você poderá entender como o ataque HTTP Request Smuggling funciona ao manipular cabeçalhos HTTP para burlar as defesas entre servidores Web através da demonstração de exemplos práticos de como explorar e mitigar essa vulnerabilidade.
09/Nov (Sab)	11:00	<b>Como o acaso nos ajuda a encontrar vulnerabilidades:</b> AFL++ e uma introdução a Feedback-Based Fuzzing	<b>Andre Bermudes</b> Tempest	O objetivo da palestra é apresentar o conceito de testes de fuzzing, sua história, e sua aplicação na busca por problemas de segurança em softwares. Além disso, serão apresentados detalhes sobre o funcionamento de um fuzzer específico, o AFL++, e ilustrado seu funcionamento através de um exemplo prático realizado em bibliotecas open-source.
	14:30	<b>Hack the Future:</b> Construindo uma Carreira e Mindset em Offensive Security	<b>Prof. Rafael Santos</b> FIAP/SP	Como explorar a mentalidade hacker e técnicas avançadas para dominar o cenário da segurança ofensiva. Com foco em estratégias de ataque, ferramentas essenciais e soft skills críticas.
	16:00	<b>Kerberos:</b> Authentication in corporate environments	<b>Jose Edgar Baccarat</b> Tempest	A apresentação abordará um protocolo de autenticação de rede desenvolvido pelo MIT (Kerberos). O Kerberos fornece segurança em sistemas distribuídos, utilizando tickets para autenticar usuários e garantir a confidencialidade das comunicações. Exploraremos seus componentes, funcionamento e alguns ataques.



Tempest

ACADEMY  
CONFERENCE <2024>

## Tempest Academy Conference 2024 | Palestras Técnicas

### Trilha: **Defensive Security**

Data	Hora	Título Palestra	Palestrante	Descrição da Palestra
08/Nov (Sex)	11:30	<b>O Alvo - Identidade Sitiada</b>	<b>Rivaldo Oliveira</b> Tempest	Vamos debater sobre as ameaças modernas que estão mirando na identidade. Visão geral sobre táticas e estratégias que os atacantes utilizam após a invasão (acesso inicial) e como você pode fortalecer suas defesas. Falaremos sobre prevenção, monitoramento e resposta.
	15:30	<b>Ciberdefesa Inteligente: Fortalecendo a Base para Proteger o Todo</b>	<b>Josué Santos</b> Tempest	Apresentar aplicação de práticas fundamentais em cibersegurança, essencial para proteger infraestruturas críticas nas grandes empresas. Ao longo da apresentação, serão abordados temas como gerenciamento de senhas, controle de acesso, atualizações de sistemas, criptografia e proteção contra-ataques de engenharia social e phishing. Serão discutidas ameaças avançadas que podem comprometer operações sensíveis, destacando a importância de uma base sólida de segurança digital para prevenir ataques cibernéticos e garantir a integridade das operações e a segurança na totalidade.
	17:00	<b>Cenários de Risco: lições cruciais dos vazamentos de dados que você não pode ignorar</b>	<b>Jessica Borges</b> Tempest	Se você quer entender como essas situações acontecem e aprender a se proteger no mundo digital, essa palestra é pra você.
	18:00	<b>Threat Hunting: Investigando o Invisível no Ciberespaço</b>	<b>Mike Garcia</b> Tempest	A palestra 'Threat Hunting - Investigando o Invisível no Ciberespaço' explora técnicas proativas para a busca de ameaças cibernéticas 'ocultas', que frequentemente ficam fora do alcance dos mecanismos de detecção.



Tempest

ACADEMY  
CONFERENCE <2024>

## Tempest Academy Conference 2024 | Palestras Técnicas

### Trilha: **Defensive Security**

Data	Hora	Título Palestra	Palestrante	Descrição da Palestra
09/Nov (Sab)	11:00	<b>Perspectivas para o cenário de inteligência cibernética</b>	<b>Daniel Nering</b> Itaú	Com o constante crescimento e mudanças das ameaças cibernéticas, precisamos constantemente criar novas soluções e técnicas para nos mantermos sempre a frente dessas ameaças. Essa palestra buscará criar esse cenário com as perspectivas para os próximos anos de como essa evolução irá ocorrer e como podemos nos preparar.
	13:30	<b>Da segurança ofensiva à defensiva: dissecando um ataque</b>	<b>Vanessa Bandeira</b> Tempest	Nesta palestra, exploraremos o ciclo completo de um ataque cibernético, desde a perspectiva ofensiva até a defensiva. Vamos dissecar cada etapa de um ataque real, mostrando as técnicas usadas por invasores para explorar vulnerabilidades e, em seguida, discutiremos como as equipes de defesa podem se proteger, detectar e mitigar essas ameaças.
	14:30	<b>Desmistificando o Trojan Bancário - Conflito Bélico de Tróia</b>	<b>Lucas Souza</b> Tempest	Essa apresentação destacaria a importância da cibersegurança no contexto financeiro e a necessidade de um constante aperfeiçoamento das medidas de proteção.
	16:30	<b>APT Groups &amp; Threat Actors no setor Aeroespacial Brasileiro</b>	<b>Rodrigo Rios</b> Tempest	O objetivo desta palestra técnica é apresentar quais são os principais grupos de ameaças persistentes avançadas (APTs) do mundo, bem como os comportamentos e o modus operandi destes grupos, suas correlações com o Estado-nação e no setor aeroespacial brasileiro e trazer uma perspectiva de defesa no contexto de Cibersegurança.
	17:30	<b>A Matrix da Mentira: Como informações manipuladas distorcem a realidade.</b>	<b>Matheus Personi</b> Tempest	Iremos mergulhar no universo da desinformação com um toque da era da inteligência artificial, explorando como a tecnologia pode ser utilizada tanto para criar quanto para combater notícias falsas. Abordaremos os impactos da desinformação no meio social com foco em exemplos práticos e casos reais. E então, entender o que podemos fazer para lidar com esse fato.



Tempest

ACADEMY  
CONFERENCE <2024>

## Tempest Academy Conference 2024 | Palestras Técnicas

### Trilha: Threat Intelligence

Data	Hora	Título Palestra	Palestrante	Descrição da Palestra
08/Nov (Sex)	15:30	<b>Dividir para escalar:</b> As principais ameaças da atual indústria do cibercrime	<b>Carlos Cabral</b> Tempest	Nesta apresentação iremos traçar um panorama sobre as principais ameaças cibernéticas do momento, destacando o caráter de interdependência entre os principais atores do cibercrime.
	17:00	<b>Do tático ao estratégico:</b> Att&ck Persistent Threat Modelling (APT Modelling)	<b>Manoelito Filho</b> Tempest	Será apresentado um framework flexível com estudo de caso a partir da identificação da capacidade de detecção do ambiente cruzada com registros históricos dos ataques realizados por grupos avançados e persistentes (APTs, do inglês Advanced Persistent Threat) através dos fundamentos e mapeamento das técnicas, táticas e procedimentos (TTPs), por segmento, para gerar a interseção entre as matrizes de capacidade de detecção (MCD) e exploração (MCE) e, assim, priorizar os esforços. O Att&ck Persistent Threat Modelling (APT Modelling) transborda e oferece uma ampla visibilidade da camada tática com intuito de otimizar a sua maturidade de cibersegurança e pode auxiliar consideravelmente na tomada de decisão na camada estratégica.
09/Nov (Sab)	11:00	<b>O que podemos descobrir sobre um binário só olhando pra fuça dele</b>	<b>Fernando Mercês</b> Mente Binária/SP	Em alguns momentos no trabalho de threat intelligence, nos deparamos com descrições de arquivos (malwares ou não) ou mesmo com capturas de tela ou vídeos onde arquivos são listados ou programas executados. O que será que dá para descobrir a partir disso? Nessa palestra vou compartilhar alguns casos reais de investigações em que fotos, vídeos e até descrições de arquivos ajudaram a encontrá-los e a enriquecer a inteligência sobre os atores.
	13:30	<b>Desvendando a Cadeia de Ataque:</b> Uma Jornada Através do Processo Investigativo de um ataque de Dupla Extorsão	<b>Ricardo Jesus</b> Tempest	Nesta sessão imersiva, os participantes serão conduzidos por uma viagem fascinante através do processo investigativo em um caso real de ataque de ransomware, que assolou uma organização de médio porte. Através de uma abordagem detalhada, guiaremos os participantes através de cada etapa do processo investigativo, desde a detecção inicial até a resolução final do incidente. Ao longo da investigação, destacamos a natureza dupla do ataque, que envolve tanto a criptografia de dados quanto a ameaça de vazamento de informações confidenciais, abordaremos também as complexidades éticas e práticas associadas à resposta a ataques de dupla extorsão, incluindo considerações sobre a conformidade regulatória, gestão de crises e tomada de decisões estratégicas. Por fim, concluiremos com insights valiosos sobre as lições aprendidas com o caso e as medidas proativas que as organizações podem adotar para fortalecer sua postura de segurança cibernética.
	16:30	<b>Engenharia Social:</b> A Arte de Manipular e Como se Proteger	<b>Cleber Castro</b> Tempest	A palestra "Engenharia Social: A Arte de Manipular e Como se Proteger" abordará tópicos referentes a quais técnicas psicológicas são usadas para manipular indivíduos e obter informações sensíveis. E nela serão discutidas estratégias utilizadas por atacantes, exemplos de golpes comuns e, principalmente, como identificar e se defender dessas ameaças, fortalecendo a segurança pessoal e corporativa.
	17:30	<b>O Papel da Inteligência de Ameaças na prevenção de ataques cibernético</b>	<b>Sidney Santana</b> Tempest	A palestra abordará a importância da inteligência de ameaças e como ela é fundamental para prever ataques, fortalecendo a defesa cibernética antes que os incidentes ocorram.



Tempest

ACADEMY  
CONFERENCE <2024>

## Tempest Academy Conference 2024 | Palestras Técnicas

### Trilha: **Infra, Cloud & IoT**

Data	Hora	Título Palestra	Palestrante	Descrição da Palestra
08/Nov (Sex)	11:30	<b>Do virtual ao chão de fábrica:</b> desvendando segurança em TI e TO	<b>Prof. Wagner Rodrigues</b> SENAI São Caetano do Sul/SP	Esta palestra explora os principais desafios na proteção de sistemas industriais contra ataques cibernéticos, com foco em ambientes de Tecnologia da Informação (TI) e Operacional (TO). Serão abordados protocolos amplamente utilizados na automação industrial e apresentados exemplos práticos de vulnerabilidades. Além disso, destacaremos a importância das normas ISO/IEC 27001 e ISA/IEC 62443 na construção de um ambiente seguro e resiliente.
	18:00	<b>O papel da Virtualização na Proteção dos Serviços Corporativos</b>	<b>Prof. Wilson Moreno</b> ABRedes/SP	O mundo está cada dia mais conectado. A necessidade de acesso à informação se faz cada dia mais urgente e crítica para a continuidade dos negócios. Proteger a informação, disponibilizar os dados e garantir a integridade desses acessos ao mesmo tempo que proporcionamos agilidade aos sistemas corporativos, se torna o grande desafio da área de Infra estrutura das empresas. Vamos falar um pouco sobre como a virtualização de serviços dessa infraestrutura pode ajudar nesse desafio de tornar os sistemas corporativos mais acessíveis, seguros e principalmente transparentes para os usuários.



Tempest

ACADEMY  
CONFERENCE <2024>

## Tempest Academy Conference 2024 | Palestras Técnicas

### Trilha: Infra, Cloud & IoT

Data	Hora	Título Palestra	Palestrante	Descrição da Palestra
09/Nov (Sab)	11:00	<b>Wi-Fi além da conectividade:</b> detecção de intrusos antecipadamente na sua rede e autenticação biométrica com Wi-Fi	<b>Prof. Lourenço Pereira</b> ITA	A utilização das funcionalidades do Wi-Fi Sensing ainda são minimamente exploradas no contexto de cibersegurança. Porém, uma tecnologia que possibilita interação com o mundo físico é bem-vinda para criação de mecanismos de proteção avançados. Esta apresentação aborda duas vertentes de aplicação do Wi-Fi Sensing: o IDS de detecção antecipada e a autenticação de sinais biométricos com Wi-Fi. Na primeira abordagem, propomos um Sistema de Detecção de Intrusão em Redes (NIDS) que emprega Sensing para identificar padrões de ataque antes que o invasor se associe à rede, utilizando modelos de aprendizado de máquina com alta precisão. Na segunda, exploramos o potencial do Wi-Fi Sensing para autenticação de usuários a partir da perturbação que as palmas das mãos dos indivíduos causa no sistema. Nossa implementação com o Raspberry Pi demonstra viabilidade de sistemas robustos de autenticação sem contato físico.
	13:30	<b>Desafios na mensuração de riscos cibernéticos:</b> Um panorama sobre as dificuldades enfrentadas na jornada de quantificação de riscos de cibersegurança	<b>Roberta Costa</b> Tempest	Vamos explorar os desafios enfrentados pelas organizações na quantificação de riscos cibernéticos. Abordaremos a natureza complexa e em constante evolução das ameaças e a dificuldade em atribuir valores monetários a ativos intangíveis. Discutiremos como a falta de métricas padronizadas e a subjetividade na avaliação de riscos dificultam o processo de tomada de decisões. Além disso, apresentaremos o conceito de TPCRM (Third-Party Cyber Risk Management), como uma estratégia crucial para mitigar riscos em um cenário onde as empresas dependem cada vez mais de fornecedores e parceiros externos. Exploraremos as melhores práticas para identificar, avaliar e gerenciar os riscos cibernéticos introduzidos por terceiros, incluindo a importância da realização de assessments, monitoramento contínuo e contratos robustos.
	14:30	<b>Votação eletrônica no Brasil:</b> desafios, perspectivas e resultados da colaboração entre TSE e academia.	<b>Prof. Marcos Simplicio</b> USP/SP	O tema de "votação eletrônica" costuma ser alvo de discussões acaloradas pelo menos a cada 2 anos no Brasil. Comumente, os argumentos utilizados envolvem pontos de crítica legítimos, meia-verdades, e também informações completamente falsas. Nesta apresentação, o objetivo é apresentar os pontos positivos e melhorias possíveis no sistema eleitoral brasileiro, fornecendo à audiência o ferramental necessário para avaliar com maior propriedade os argumentos a favor e contra os mecanismos atuais. Ao mesmo tempo, são discutidos os resultados da colaboração existente entre TSE e pesquisadores de universidades brasileiras nos últimos 4 anos, que buscam trazer melhorias à segurança, transparência, usabilidade e custos do sistema. Como um bônus, são analisadas do ponto de vista técnico algumas das principais alegações de fraude nas eleições de 2022.
	16:00	<b>O poder da simplicidade na era hiperconvergente</b> – Por que complicar, se o arroz com feijão ainda sustenta?	<b>Prof. Luciano Peraro</b> CPS ETEC/SP	Nesta apresentação irei abordar questões de como as boas práticas de verificação, gestão de mudança e aplicação de patches no tempo correto nas plataformas de virtualização e hiperconvergência permeiam a manutenibilidade de um ambiente produtivo e sem incidentes.



Tempest

ACADEMY  
CONFERENCE <2024>

Tempest Academy Conference 2024 | Palestras Técnicas

Trilha: Engenharia de Software & Data Science(DS)/Artificial Intelligence(AI)/Machine Learning(ML)

Data	Hora	Título Palestra	Palestrante	Descrição da Palestra
08/Nov (Sex)	11:30	<b>O Impacto da Inteligência Artificial Generativa em Resolver Issues de Código em Ambientes DevSecOps</b>	<b>Prof. Cesar Marcondes</b> ITA/SP	<p>A crescente adoção de práticas DevOps tem impulsionado a busca por maior agilidade e eficiência no desenvolvimento de software. Nesse contexto, a inteligência artificial generativa (GenAI) emerge como um catalisador, transformando significativamente o processo de revisão de código. Esta palestra abordará o estado da arte em geração de código para pull requests, com foco no papel de ferramentas como Aider, SWE-Bench e Devin. Estas ferramentas vão além da simples geração de código, oferecendo análises críticas e sugestões automatizadas que elevam a qualidade do software.</p> <p>Serão explorados os benefícios da integração da GenAI nos fluxos de trabalho de DevSecOps, demonstrando como a automação impulsionada por IA acelera os ciclos de desenvolvimento e aprimora a colaboração entre as equipes de desenvolvimento e operações. A ferramenta SWE-Bench será detalhadamente apresentada, com ênfase na visualização das trajetórias de um issue de github até um pull request completo por IA, permitindo uma compreensão mais profunda de como estas tecnologias influenciam o desenvolvimento ao longo do tempo. Adicionalmente, serão discutidas as vantagens da utilização dessas ferramentas para automatizar revisões de código, reduzir a incidência de erros humanos e, consequentemente, entregar produtos de software mais robustos e inovadores.</p> <p>Por fim, a palestra abordará as perspectivas futuras da integração da GenAI em DevOps, projetando um cenário onde a inteligência artificial desempenha um papel cada vez mais central na otimização dos processos de desenvolvimento, assegurando a competitividade e a qualidade na era digital.</p>
	15:30	<b>Data Science &amp; IA:</b> Education First	<b>Marco Carvalho</b> ABRedes   Matza/RJ	<p>Nunca da história da humanidade tivemos tanto acesso a dados e a ferramentas que geram valor de negócios com sua análise. Desde a estatística nos tempos de bancos relacionais, passando pelo data warehouse com bancos tabulares, dos dados não estruturados avaliados com Map Reduce, até os dias de hoje com IA Generativa e seus LLMs.</p> <p>No entanto, mesmo com este verdadeiro arsenal de tecnologia, o mundo de negócios parece não conseguir tracionar. O que está faltando?</p> <p>Qual o caminho para se conseguir gerar valor para os negócios com tecnologia?</p> <p>Nesta palestra vamos abordar a relevância da educação como premissa, ou a abordagem Education First, que coloca o ser humano no centro, como o protagonista dos negócios, usando estas ferramentas para otimizar sua atuação.</p>
	17:00	<b>IA Generativa:</b> Aplicações e Preocupações	<b>Carlos Guerra</b> Embraer	<p>Após o boom das IAs Generativas, estamos testemunhando uma vasta gama de aplicações dessa tecnologia. Esta apresentação oferece uma contextualização histórica, destaca as principais ferramentas disponíveis e exemplos práticos de uso. Também aborda algumas preocupações relacionadas ao emprego dessa tecnologia.</p>
	18:00	<b>Inteligência Artificial e Cibersegurança para Transformação Digital</b>	<b>Prof. Sanval Ebert &amp; Leonardo Cardia</b> CIMATEC/BA	<p>A palestra abordará como a IA pode influenciar o campo da cibersegurança e contribuir para a transformação digital. Serão discutidas as possibilidades de integrar IA em estratégias de segurança para automatizar processos, prever ameaças e aprimorar a resposta a incidentes. Além disso, será explorada a criação de uma visão estratégica para fortalecer a segurança digital e impulsionar a transformação digital nas organizações.</p>



Tempest

ACADEMY  
CONFERENCE <2024>

## Tempest Academy Conference 2024 | Palestras Técnicas

Trilha: **Engenharia de Software & Data Science(DS)/Artificial Intelligence(AI)/Machine Learning(ML)**

Data	Hora	Título Palestra	Palestrante	Descrição da Palestra
	13:30	<b>Subvertendo Modelos de Machine Learning com Ataques Adversariais</b>	<b>Paulo Matana</b> Tempest	Modelos de aprendizagem de máquina têm sido amplamente empregados nas mais diversas aplicações: de sistemas de autenticação a veículos autônomos, de plataformas de streaming a aplicativos de venda de passagens aéreas. Mas, apesar dos seus bons resultados, será que usar modelos de aprendizagem de máquina é seguro? Nesta palestra, iremos mostrar que o uso desses modelos introduz novos riscos e vulnerabilidades, pois uma categoria de ataques chamada de ataques adversariais pode subverter o funcionamento de modelos de aprendizagem de máquina e induzi-los ao erro. Por fim, também discutiremos e faremos recomendações sobre como mitigar estes tipos de ataques.
	14:30	<b>NLP e Assistentes Virtuais de Voz:</b> Processamento de Linguagem Natural na Prática: Entendendo o Funcionamento por traz da Alexa	<b>Douglas Oliveira</b> Tempest	De comandos simples a tarefas complexas, a Alexa demonstra o poder do Processamento de Linguagem Natural (PNL) em nosso dia a dia. Nesta palestra, desvendaremos os mecanismos por trás dessa tecnologia, explorando como a Alexa reconhece nossa fala, interpreta comandos e gera respostas em áudio. Abordaremos os principais conceitos de NLP, exemplos práticos de seu uso, além de discutir os desafios e avanços nesse campo em constante evolução.
	17:00	<b>Do Vale da Estranheza à Conquista da Cibersegurança:</b> Formação, Talentos e Mindset na Era da Inteligência Artificial.	<b>Profª. Olivia Braga</b> FIAP/SP	Nesta palestra, vamos explorar a jornada de superação do Vale da Estranheza no campo da cibersegurança e como a Inteligência Artificial (IA) está transformando essa área crítica. O conceito de Vale da Estranheza é usado metaforicamente para ilustrar os desafios iniciais enfrentados por estudantes e profissionais ao adentrar o mundo da cibersegurança e IA, onde a complexidade e a falta de familiaridade podem gerar desconforto. Açou estranho? Vamos falar sobre isso?



Tempest

ACADEMY  
CONFERENCE <2024>

## Tempest Academy Conference 2023 | Minicursos

Trilha	Data	Hora	Título do Mini-Curso	Instrutor	Descrição do Mini-Curso
Offensive	08/Nov (Sex)	10:30 às 19:00	<b>Introdução à Web Application Security para futuros pentesters</b>	<b>Gabrielle Delgado &amp; Jéssica Guiot</b> Tempest	<p><b># OBJETIVO GERAL:</b> Apresentar as bases, táticas e técnicas voltados ao pentest de aplicações web, utilizando materiais de referência e laboratórios online através dos fundamentos sobre vulnerabilidades comuns voltadas à aplicações web. Participantes poderão ensaiar algumas técnicas iniciais comumente utilizadas em missões de pentest web profissionais.</p> <p><b># METODOLOGIA:</b> Apresentação de conceitos por meio de slides e execução dos conceitos em ambiente online para prática de testes.</p> <p><b># CONTEÚDO PROGRAMÁTICO:</b> - Introdução aos princípios básicos de segurança - Fundamentos sobre tecnologias web - Utilização do Burp Suite para exploração de vulnerabilidades - Conceito e exploração de falhas em: * Token de sessão previsível; * Ausência de mecanismos antiautomação; * Enumeração de usuários; * Cross-Site Scripting (XSS); * Injeção de comandos SQL, entre outras -Caminhos para continuar evoluindo no assunto</p> <p><b># CARGA HORÁRIA:</b> 7 horas</p> <p><b># PRÉ-REQUISITOS:</b> <b>Conhecimentos prévios:</b> É necessário ter alguma experiência em interação com aplicações web. Ter conhecimentos básicos de programação web será um facilitador para a compreensão do conteúdo. Ter utilizado o GitHub pelo menos uma vez também será útil. <b>Linguagem de programação:</b> O minicurso não é focado em desenvolvimento, mas, se necessário, poderá ser utilizado o Python durante as aulas. <b>Sistemas operacionais:</b> Não há a exigência de um sistema operacional específico. <b>Outros conhecimentos técnicos relevantes:</b> Saber utilizar ferramentas de desenvolvimento dos navegadores pode ser</p> <p><b>#PRÉ-REQUISITOS: DE EQUIPAMENTOS:</b> <b>Configuração mínima:</b> Qualquer máquina com pelo menos 2 núcleos de processamento e 8GB de RAM será suficiente para realizar as atividades básicas, como executar um navegador e um proxy (Burp Suite). <b>Softwares necessários:</b> Um navegador e o Burp Suite Community. Os participantes que desejarem replicar os exemplos durante o minicurso precisarão desses programas instalados. <b>Conectividade à internet:</b> É necessário ter acesso à internet para acessar os conteúdos práticos durante o minicurso. O material poderá ser acessado posteriormente, em casa, se necessário.</p>



Tempest

ACADEMY  
CONFERENCE <2024>

### Tempest Academy Conference 2023 | Minicursos

Trilha	Data	Hora	Título do Mini-Curso	Instrutor	Descrição do Mini-Curso
Artificial Intelligence / Data Science / Machine Learning	08/Nov (Sex)	10:30 às 19:00	<b>Empowering Intrusion Detection Systems with Machine Learning</b>	<b>Paulo Matana &amp; Julio Luz</b> Tempest	<p><b># OBJETIVO GERAL:</b></p> <ul style="list-style-type: none"><li>- Demonstrar como a aprendizagem de máquina (machine learning – ML) pode fortalecer sistemas de detecção de intrusão (intrusion detection systems – IDS) e permitir a detecção de ataques cibernéticos mais complexos.</li><li>- Abordaremos, de maneira prática e com atividades hands-on, as principais técnicas de aprendizagem utilizadas em IDSs do estado da arte, bem como os conceitos essenciais de machine learning para facilitar a compreensão dessas técnicas.</li></ul> <p><i>Obs.: Para participar do minicurso no formato presencial, há a necessidade de levar o seu notebook pessoal.</i></p> <p><b># METODOLOGIA:</b></p> <p>Apresentação do conteúdo por meio de slides e demonstrações em tempo real, visando a aplicação prática em ambiente online para realização de testes.</p> <p><b># CONTEÚDO PROGRAMÁTICO:</b></p> <p>Capítulo 1 - A Connected World:</p> <ul style="list-style-type: none"><li>- Motivação para o uso de sistemas de detecção baseados em anomalia e introdução básica a taxonomia de sistema de detecção de intrusão.</li></ul> <p>Capítulo 2 - Anomaly-based Detection:</p> <ul style="list-style-type: none"><li>- Introdução ao conceito de detecção de anomalia e a necessidade do uso de aprendizagem de máquina;</li><li>- Como definir quais dados usar em um projeto de IDS baseado em anomalias;</li><li>- [Hands-on]: Preparação e análise de dados.</li></ul> <p>Capítulo 3 - Machine Learning gets Involved:</p> <ul style="list-style-type: none"><li>- Modelos clássicos de ML para detecção de anomalias;</li><li>- [Hands-on]: Clustering;</li><li>- Deep learning: Introdução e nivelamento de conhecimento;</li><li>- Autoencoders;</li><li>- [Hands-on]: Autoencoders;</li></ul> <p>GANs;</p> <p>[Hands-on]: GANs.</p> <p>Capítulo 4 - From Theory to Practice: ML-Based IDSs in the Real World:</p> <ul style="list-style-type: none"><li>- Onde IDS baseados em ML são usados no mundo real;</li><li>- Como a Tempest utiliza essas tecnologias;</li></ul> <p><b># CARGA HORÁRIA:</b></p> <p>- 7 horas</p> <p><b># PRÉ-REQUISITOS DE CONHECIMENTO TÉCNICO</b></p> <ul style="list-style-type: none"><li>- Para conseguir acompanhar confortavelmente o conteúdo do minicurso, é desejável, sobretudo, que o participante tenha noções básicas de machine learning.</li></ul> <p><b># REQUISITOS DE EQUIPAMENTO</b></p> <ul style="list-style-type: none"><li>- Necessário computador/notebook ou VM com S.O Windows instalado;</li><li>- Para o bom andamento da aula prática, o plano gratuito do Google Colab será o suficiente. De tal forma, não será necessário mais do que apenas um navegador para conseguir trabalhar com os códigos sem problemas.</li><li>- Caso o participante faça questão de usar um ambiente local em seu notebook, será necessário ter, pelo menos, uma configuração com 8GB de RAM e um processador Core i5 ou Ryzen5 recente.- Acesso a Internet</li></ul>



Tempest

ACADEMY  
CONFERENCE <2024>

## Tempest Academy Conference 2023 | Minicursos

Trilha	Data	Hora	Título do Mini-Curso	Instrutor	Descrição do Mini-Curso
Offensive	09/Nov (Sab)	10:00 às 14:00	Introdução a engenharia reversa de software	Gustavo Andia Carvalho Tempest	<p><b># OBJETIVO GERAL:</b></p> <ul style="list-style-type: none"><li>- Compreender os fundamentos básicos da engenharia reversa por meio da análise de executáveis e crackmes, com o objetivo final de analisar um desafio e desenvolver um keygen em Python.</li><li>- Abordaremos de forma prática, com atividades hands-on, tópicos relacionados a representações numéricas, criação e análise de executáveis em assembly, o formato PE, crackmes e, por fim, o desenvolvimento de um keygen para solucionar o desafio final.</li></ul> <p>Obs.: Para participar do minicurso no formato presencial, há a necessidade de levar o seu notebook pessoal.</p> <p><b># METODOLOGIA:</b></p> <p>O conteúdo será apresentado por meio de slides e demonstrações em tempo real, onde o conteúdo básico será apresentado e os exercícios resolvidos ao vivo.</p> <p><b># CONTEÚDO PROGRAMÁTICO:</b></p> <ul style="list-style-type: none"><li>- Representações numéricas (binário, decimal, hexadecimal)</li><li>- O básico da linguagem Assembly</li><li>- O que é um compilador.</li><li>- Formato PE</li><li>- Debugger (x64dbg)</li><li>- Crackmes</li><li>- Desafio final (keygen de um crackme em python)</li><li>- Demonstração da análise de um malware.</li></ul> <p><b># CARGA HORÁRIA</b></p> <p>4 horas</p> <p><b># PRÉ-REQUISITOS DE CONHECIMENTO TÉCNICO</b></p> <ul style="list-style-type: none"><li>- Para conseguir acompanhar o conteúdo do minicurso, é desejável, sobretudo, que os participantes tenham noções básicas de programação.</li></ul> <p><b># REQUISITOS DE EQUIPAMENTO</b></p> <ul style="list-style-type: none"><li>- É necessário um computador ou notebook com o sistema operacional Windows instalado.</li><li>- O VirtualBox deve estar instalado com a máquina virtual do minicurso devidamente configurada.</li></ul> <p>Obs.:</p> <ul style="list-style-type: none"><li>- O computador deve atender aos requisitos mínimos para executar o Windows e uma máquina virtual emulada pelo VirtualBox.</li><li>- O link para download da máquina virtual do minicurso estará disponível, neste documento, 1 semana antes do início do treinamento</li></ul> <p>Link para download da máquina virtual do minicurso : <a href="https://drive.google.com/file/d/15jUseTo2Nv3lx8IYAfjCSLN2M1e1CVV/view?usp=sharing">https://drive.google.com/file/d/15jUseTo2Nv3lx8IYAfjCSLN2M1e1CVV/view?usp=sharing</a></p>



Tempest

ACADEMY  
CONFERENCE <2024>

## Tempest Academy Conference 2023 | Minicursos

Trilha	Data	Hora	Título do Mini-Curso	Instrutor	Descrição do Mini-Curso
Threat Intel	09/Nov (Sab)	10:00 às 14:00	<b>OpenCTI na Prática: Fortalecendo a Segurança com Inteligência de Ameaças</b>	<b>Prof. José Marivaldo Aragão da Silva</b> CIMATEC BA	<p><b># OBJETIVO GERAL:</b> - Apresentar um guia detalhado e prático para a implementação e uso estratégico do OpenCTI em uma organização, desde a configuração inicial até a integração com outras ferramentas de segurança, com foco em superar desafios comuns. Ao final do minicurso, os participantes terão uma compreensão sólida sobre a utilização do OpenCTI em cenários reais e estratégias para otimização contínua.</p> <p><b># METODOLOGIA:</b> - Apresentação do conteúdo por meio de slides e demonstrações em tempo real, visando a aplicação prática em ambiente online para realização de testes.</p> <p><b># CONTEÚDO PROGRAMÁTICO:</b> - Introdução ao OpenCTI, - Preparação para a Implementação, - Configuração do OpenCTI, - Uso Prático do OpenCTI, Colaboração e Compartilhamento de Dados, - Conclusão e Próximos Passos.</p> <p><b># CARGA HORÁRIA</b> 4 horas</p> <p><b># PRÉ-REQUISITOS DE CONHECIMENTO TÉCNICO</b> - Conhecimento básico em segurança da informação, Familiaridade com conceitos de inteligência de ameaças e Noções de integração de APIs e ferramentas de segurança.</p> <p><b># REQUISITOS DE EQUIPAMENTO</b> Configurações mínimas do computador: - Processador de 4 cores ou superior; - Memória RAM de 4GB ou superior; - Espaço disponível em disco de 30GB; - VirtualBox (6.1 ou superior) ou VMware (16 ou superior). A tecnologia de virtualização da BIOS deve estar habilitada e será necessário acesso à Internet.</p>



Tempest

ACADEMY  
CONFERENCE <2024>

## Tempest Academy Conference 2023 | Minicursos

Trilha	Data	Hora	Título do Mini-Curso	Instrutor	Descrição do Mini-Curso
Cloud Sec	09/Nov (Sab)	14:00 às 18:00	Introdução a segurança na plataforma Google Cloud	João Marcos Leite ABRedes   Matza	<p><b># OBJETIVO GERAL:</b></p> <ul style="list-style-type: none"><li>- Compreender a abordagem da Google Cloud para segurança e os mecanismos de defesa em profundidade;</li><li>- Entender quais medidas podem ser adotadas para prevenir ataques DDoS e mitigar diversos cenários de vulnerabilidades;</li><li>- Realizar hands-on na console Security Command Center da plataforma Google Cloud para implementar controles de acesso.</li></ul> <p>OBS1.: Para participar do minicurso no formato presencial, há a necessidade de levar o seu notebook pessoal.</p> <p>OBS2.: Para conseguir realizar as atividades hands-on previstas no dia do curso é <b>OBRIGATORIAMENTE necessário</b> que você <b>se inscreva gratuitamente até dia 04/Nov</b> no programa <b>Google Arcade Facilitator</b> por meio do link abaixo: <a href="https://bit.ly/ARCADE-TEMPEST">https://bit.ly/ARCADE-TEMPEST</a></p> <p>BONUS: Os participantes deste minicurso que estejam inscritos no Google Cloud Arcade Facilitator terão acesso GRATUITO por 6 meses aos laboratórios oficiais do Google Cloud Skills Boost (que normalmente custam US\$200/semestre).</p> <p><b># METODOLOGIA:</b></p> <ul style="list-style-type: none"><li>- O conteúdo teórico será apresentado por meio de slides;</li><li>- A parte hands-on será realizada pelos participantes através de laboratórios práticos na plataforma oficial de treinamento Google Cloud Skills Boost.</li></ul> <p><b># CONTEÚDO PROGRAMÁTICO:</b></p> <ul style="list-style-type: none"><li>- Fundamentos de segurança da Google Cloud</li><li>- Cloud Identity e Identity and Access Management (IAM)</li><li>- Configurando a rede Virtual Private Cloud para isolamento e segurança</li><li>- Segurança de recursos computacionais e aplicações</li><li>- Segurança dos dados na nuvem</li><li>- Protegendo-se contra ataques e mitigando vulnerabilidades</li><li>- Monitoring, Logging, Auditing e Scanning</li><li>- Entendendo e usando o Security Command Center</li></ul> <p><b># CARGA HORÁRIA:</b></p> <ul style="list-style-type: none"><li>- 04 horas</li></ul> <p><b># PRÉ-REQUISITOS DE CONHECIMENTO TÉCNICO</b></p> <ul style="list-style-type: none"><li>- Para conseguir acompanhar o conteúdo do minicurso, é desejável que o participante tenha conhecimentos básicos de segurança da informação.</li><li>- Proficiência básica em ferramentas de linha de comando e sistema operacional Linux.</li></ul> <p><b># REQUISITOS DE EQUIPAMENTO</b></p> <ul style="list-style-type: none"><li>- É necessário o sistema operacional Windows e um browser web instalado.</li></ul> <p><b>DUVIDAS:</b> Em caso de dúvidas envie um e-mail para <a href="mailto:arcade@matza.academy">arcade@matza.academy</a></p>



Tempest

ACADEMY  
CONFERENCE <2024>

### CyberSec Jobs - Empresa Participante | Programação

#### EMBRAER

Data	Hora	Título Palestra	Palestrante	Descrição da Palestra	Modalidade/Local
08/Nov (Sex)	Dia Todo	<b>Bate Papo com o time de Atração de Talentos da Embraer</b>	Diversas Pessoas	O time de Atração de Talentos, estará disponível no Stand da Embraer durante todo o dia para networking, dúvidas e dicas .	<b>Presencial:</b> Stand
	10:30 às 11:00	<b>Oportunidades do Programa de Especialização em Software da Embraer</b>	Marcelo Ruy & Convidados da Embraer	Neste bate papo será abordado as principais oportunidades ofertadas pela Embraer em seu PES - Programa de Especialização em Software, onde participantes do PES estarão comentando sobre os benefícios e vantagens que eles conseguem obter por fazerem parte deste ótimo programa de formação técnica para atuação profissional na Embraer.	<b>Híbrido:</b> Presencial: Auditório Remoto: Zoom
	15:00 às 16:00	<b>Embraer: Roda de Conversa</b>	Carlos Guerra, Manuela Souza & Iraline Nunes/Embraer	A Embraer irá promover uma roda de conversa com participantes de seus programas de formação técnica, visando apresentar grandes oportunidades que estudantes que estão se preparando para a entrada no mercado profissional podem se beneficiar.	<b>Híbrido</b> Presencial: Sala 101D Remoto: Zoom

### CyberSec Jobs - Empresa Participante | Programação

#### ITAU

Data	Hora	Título Palestra	Palestrante	Descrição da Palestra	Modalidade/Local
08/Nov (Sex)	Dia Todo	<b>Bate Papo com o time de Atração de Talentos do Itaú</b>	Diversas Pessoas	O time de Atração de Talentos, estará disponível no Stand do Itaú durante todo o dia para networking, dúvidas e dicas .	<b>Presencial:</b> Stand
	15:30 às 16:30	<b>Itaú: Papo com Itaú: Carreiras &amp; Programa de Estágio</b>	Wallace Santos/Itaú & Leandro Jordino/Itaú	Conheça o ecossistema Itaú Unibanco, nossos programas de entrada, cultura e dia a dia da pessoa na carreira de Cyber.	<b>Híbrido</b> Presencial: Sala 101D Remoto: Zoom
09/Nov (Sáb)	10:00 às 10:30	<b>Roda de Conversa: Cultura &amp; Carreiras</b>	Ineida Moura & Convidados/Itaú	Conheça um pouco da empolgante e dinâmica cultura interna do Itaú Unibanco e das possibilidades de atuação profissional e das trilhas de carreiras que existem dentro do time de Cibersegurança e Tecnologia da Informação.	<b>Híbrido</b> Presencial: Auditório Remoto: Zoom



Tempest

ACADEMY  
CONFERENCE <2024>

### CyberSec Jobs - Empresa Participante | Programação

TEMPEST

Data	Hora	Título Palestra	Palestrante	Descrição da Palestra	Modalidade/Local
08/Nov (Sex)	Dia Todo	<b>Bate Papo com o time de Atração de Talentos da Tempest</b>	Diversas Pessoas	O time de Atração de Talentos, estará disponível no Stand da Tempest durante todo o evento para networking, dúvidas e dicas .	<b>Presencial:</b> Stand
	15:00 às 15:30	<b>Quer conhecer mais o Time de Atração de Talentos da Tempest ?</b>	Suellen Oliveira, Ana Emília e Roberto Alexandre	Nesta apresentação falaremos um pouco sobre a atuação da área de Atração de Talentos da Tempest, bem como de suas iniciativas e projetos. Ao final faremos um convite para participação nos demais momentos da agenda de atividades da Tempest no CyberSec Jobs e ainda faremos uma surpresa ao final.	<b>Híbrido</b> Presencial: Auditório Remoto: Zoom
	17:00 às 18:00	<b>Venha conhecer o Programa de Estágio da Tempest</b>	Suellen Oliveira, Ana Emília e Roberto Alexandre	Um espaço reservado para apresentar a vocês o nosso programa de estágio, mostrar um pouco sobre como é o nosso processo, acompanhamento durante todo o estágio. Nesse papo teremos gestores e estagiários que vão falar como é a sua experiência e, claro, vão rolar aquelas dicas maravilhosas para vocês se prepararem.	<b>Híbrido</b> Presencial: Sala 101D Remoto: Zoom
09/Nov (Sab)	Dia Todo	<b>Bate Papo com o time de Atração de Talentos da Tempest</b>	Suellen Oliveira, Ana Emília e Roberto Alexandre	O time de Atração de Talentos, estará disponível durante o evento para dúvidas e dicas .	<b>Presencial:</b> Stand
	16:00 às 17:00	<b>Roda de Conversa - Carreiras: O jeito Tempester de Ser (pensar mais)</b>	Convidados: 3 colaboradores Tempest. [Especialistas]	Vamos trazer um momento de bate-papo com alguns dos nossos colaboradores de áreas diversas, para trazer na visão do Tempester, como é fazer parte da nossa Jungle, como é a cultura Tempest, além de muitas dicas sobre carreira, estudos e muito mais.	<b>Híbrido</b> Presencial: Sala 101D Remoto: Zoom



## Capture the Flag (Presencial ou Remota)

Durante o Evento também será promovido uma competição no formato Capture the Flag (CtF), através de desafios estimulantes e divertidos, como mais uma oportunidade para o desenvolvimento de algumas habilidades técnicas que podem vir contribuir na formação da competência profissional em cibersegurança. Interessados deverão competir com seus próprios notebooks e concorrerão a premiações no final da competição.

## CyberSec Jobs (Feira de Empregabilidade para Talentos)

Ao longo da realização do Evento, a Tempest e algumas de suas empresas parceiras, irão estar com seus times de Atração de Talentos organizando várias atividades junto aos participantes (presenciais e remotos), tais como: sorteio de brindes, levantamento e análise de currículos, mapeamento de talentos profissionais, orientações sobre programas de estágios e possíveis entrevistas para ofertas de oportunidades e vagas profissionais.



Tempest

ACADEMY  
CONFERENCE <2024>

### **Ask the Experts:**

Durante todo o evento, em um ambiente exclusivo aos participantes inscritos apenas na modalidade presencial, Consultores Técnicos experientes da Tempest estarão disponíveis para uma interação 1:1 (one on one) com estudantes e professores(as) visando tirar dúvidas técnicas, trocar experiências profissionais ou prestar orientações técnicas sobre questões relacionadas às suas áreas de especialidades em cibersegurança.

### **Reunião Professores(as) do ACTION Talents:**

Será realizado uma reunião especial somente aos Professores(as) participantes da Conferência (presenciais ou remotos) que vêm atuando na validação do piloto deste programa educacional da Tempest ao longo de 2024. O objetivo será que estes professores(as) possam apresentar e compartilhar com os demais colegas as boas práticas e os seus bons resultados alcançados em todo o Brasil através do uso dos recursos do ACTION Talents.

Datas: **8 e 9/Nov/2024**

Local: **Universidade São Judas - Móoca (São Paulo/SP)**

Formato: **Híbrido**



**Tempest**

**ACADEMY**  
**CONFERENCE < 2024 >**

Inscrições pelo Even3:



**[even3.com.br/tempest-academy-conference-2024/](https://even3.com.br/tempest-academy-conference-2024/)**



**Tempest**